Privacy by design prevents data headaches later

Nancy Dickie and Andrew Yule

Little more than a year remains before the General Data Protection Regulation (GDPR) comes into force.

Many larger businesses and those operating in the technology and data sectors are likely to already be pretty *au fait* with existing data protection matters and may feel reasonably well prepared for GDPR. But complacency can be dangerous – and it is probably fair to say that many businesses have traditionally taken a fairly reactive approach, with no-one truly taking ownership of ensuring that data protection principles are embedded within their organisation.

Under the GDPR, a passive or reactive approach will not pass muster and will potentially expose any business to an intimidating fines regime.

So, where should HR practitioners start with GDPR? The first step is a conceptual one. Accept that personal data are not something or somewhere else, rather it is engrained in everything your business does – particularly where people are at the heart of the business model (or, of that part of it in which you operate). The GDPR recognises this concept by demanding that data privacy rights are factored into every aspect of your business, where people and their data are involved.

So, just as HR professionals embrace the fact that every decision they make and every policy they implement must be assessed through the lens of discrimination laws – so, they must now get used to applying a GDPR lens to everything the business plans and does, which affects or that may involve the processing of employees' (or anyone else's) personal data. This is what we mean by privacy by design.

Privacy by design

The concept of "privacy by design" is not new. The UK regulator (the ICO) has recommended the approach as best practice for some time. However, the GDPR goes further – it bakes it into the letter of the law.

Personal data implications can no longer be treated as a discrete element of or a bolt-on to an internal project. Privacy by design demands that you are proactive in addressing the privacy implications of any new or upgraded system, procedure, policy or data-sharing initiative, throughout its planning phase and its full lifecycle. Indeed, it is important to note that GDPR couches privacy by design as an approach to take both at the outset of a project or system and during its operation, again highlighting that data protection considerations are

Nancy Dickie is based at Winckworth Sherwood LLP, London, UK. Andrew Yule is Partner at Winckworth Sherwood LLP, London, UK.

more than a box to be ticked before moving on.

This means that HR cannot work (or be expected to work) in isolation. To be GDPR compliant, every aspect of the business that potentially relies on or processes employees' personal data, should be considered from a privacy perspective: what data will be processed; why; how and where will it be stored; who will it be accessible to and why; is it up-to-date and accurate; how long will you keep it for; how will it be protected; and how is all of this justified? At the very least, HR will need the cooperation and support of colleagues in information technology, procurement (particularly where external systems may be used), legal and of course engagement from senior management.

Data Protection Impact Assessments (DPIAs) are also a practical way to implement privacy by design, and the GDPR specifically mentions that data processing using "new technologies" should be subjected to a DPIA – examples of activities that are caught by the provision include the processing of substantial amounts of sensitive personal data (such as health or genetic information), systematic profiling (for example that carried out by insurance providers) and large-scale CCTV operations. We await further guidance from supervisory authorities, but we do know that a DPIA should involve a detailed specification of the relevant system or operations, assessing the risk to individuals' privacy rights and the necessity and proportionality of the planned processing. Bear in mind also that under GDPR there is an emphasis on governance and accountability: it will not be enough to comply with the rules. Businesses will also need to be able to demonstrate how they are complying.

This also leads to another core GDPR concept – "privacy by default". As well as considering how data will be used, it will be necessary to undertake a thorough assessment of whether it is genuinely needed and for how long it needs to be retained.

This may all mean additional time and resources, particularly at the front-end of and when upgrading and designing systems. But this will inevitably be more cost-effective than turning a blind eye now, then grappling with having to re-engineer systems once they are in place – not to mention having been stung by the harsh sanctions regime that accompanies the GDPR.

Be prepared

The GDPR may seem like climbing a compliance mountain, with only a short time left to "get fit". But as is so often the case, it is the first training run that is intimidating – and there are many things you can do now to start to prepare and once you have started, the slope will soon start to feel less steep:

- Gather information: what data do you routinely hold (from an HR perspective, we are largely talking about employees' data – but do not forget candidates, ex-employees, consultants and others). Where is it gathered from, on what basis and who is it shared with? A data-mapping exercise is a good place to start and will highlight areas which may need more detailed attention, for example planned new systems or products that would benefit from a DPIA.
- Review systems and processes: how can they support the need for accountability and therefore reduce the compliance burden for your data-protection officer? If a new system is planned – even if before GDPR comes into force – use privacy by design and default to ensure no substantial changes are necessary after May 2018.
- Do you have a budget for GDPR compliance? With finances stretched for many businesses, use the results of your data mapping and other activity to identify high-risk activities that may well benefit from both additional resources.
- Ensure that you have conversations across your organisation to gain senior level buy-in. GDPR demands a holistic approach.

Corresponding author

Andrew Yule can be contacted at: ayule@wslaw.co.uk